

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Naoki NIMURA et al.

Application No.: NEW

Group Art Unit: Not Yet Assigned

Filed: February 25, 2004

Examiner: Not Yet Assigned

For: FILE SECURITY MANAGEMENT METHOD AND FILE SECURITY MANAGEMENT APPARATUS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-95722

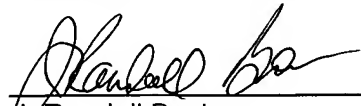
Filed: March 31, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 25, 2004

By: 
Randall Beckers
Registration No. 30,358

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: March 31, 2003

Application Number: Patent Application No. 2003-095722
[ST.10/C] [JP2003-095722]

Applicant(s): FUJITSU LIMITED

December 9, 2003

Commissioner,

Japan Patent Office Yasuo IMAI

Certificate No. P2003-3101649

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 3 1 日
Date of Application:

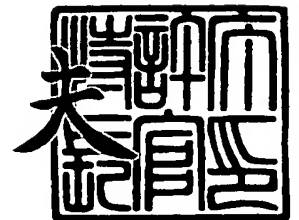
出 願 番 号 特 願 2 0 0 3 - 0 9 5 7 2 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 9 5 7 2 2]

出 願 人 富士通株式会社
Applicant(s):


2 0 0 3 年 1 2 月 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 1 0 1 6 4 9



【書類名】 特許願

【整理番号】 0350256

【提出日】 平成15年 3月31日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 ファイルのセキュリティ管理プログラム及びファイルの
セキュリティ管理装置

【請求項の数】 5

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

 【氏名】 二村 直樹

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

 【氏名】 河野 太基

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100074099

 【住所又は居所】 東京都千代田区二番町 8 番地 2 0 二番町ビル 3 F

 【弁理士】

 【氏名又は名称】 大菅 義之

 【電話番号】 03-3238-0031

【選任した代理人】**【識別番号】** 100067987**【住所又は居所】** 神奈川県横浜市鶴見区北寺尾 7-25-28-503**【弁理士】****【氏名又は名称】** 久木元 彰**【電話番号】** 045-573-3683**【手数料の表示】****【予納台帳番号】** 012542**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9705047**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 ファイルのセキュリティ管理プログラム及びファイルのセキュリティ管理装置

【特許請求の範囲】

【請求項 1】 ファイルのセキュリティ管理プログラムにおいて、コンピュータに、

ファイルを開くことのできる位置を指定する位置情報をキーとして前記ファイルを暗号化する暗号化手段と、

前記位置情報をキーとして暗号化されたファイルを保存する保存手段と、

位置検出手段により検出される位置情報をキーとしてファイルを復号する復号化手段と、

前記復号化手段により復号されたファイルを表示する表示手段として機能させるためのセキュリティ管理プログラム。

【請求項 2】 請求項 1 記載のファイルのセキュリティ管理プログラムであって、

前記暗号化手段は更に、ファイルを復号することが可能な位置情報の選択時に予め登録してある複数箇所の中から選択することを特徴とするセキュリティ管理プログラム。

【請求項 3】 請求項 1 記載のファイルのセキュリティ管理プログラムであって、

前記暗号化手段は更に、暗号化のキーとして用いる位置情報のデータ長を変化させることで前記ファイルを開くことのできる範囲を限定することを特徴とするセキュリティ管理プログラム。

【請求項 4】 ファイルのセキュリティ管理プログラムにおいて、

利用できる位置を指定する位置情報をキーとしてデータを暗号化した暗号化済データを有し、

コンピュータに、

予めファイルを開くことのできる位置が指定された位置情報をキーとして保存しておき、

位置検出手段により検出される位置情報に基づき、前記キーと合致するか否かを判定し、合致する場合は前記暗号化済データを復号する復号化手段と、

前記復号化手段により復号されたデータを表示する表示手段
として機能させるためのセキュリティ管理プログラム。

【請求項 5】 ファイルのセキュリティ管理装置において、
ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化する暗号化手段と、

前記位置情報をキーとして暗号化されたファイルを保存する保存手段と、
位置検出手段により検出される位置情報をキーとしてファイルを復号する復号化手段と、

前記復号化手段により復号されたファイルを表示する表示手段
とを備えることを特徴とするセキュリティ管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ファイルのセキュリティ管理プログラム及びセキュリティ管理装置に関する。

【0002】

【従来の技術】

インターネット等のネットワークの普及によりネットワークを介してユーザがシステムをアクセスできるようになっている。一般に、システムに対する不正なアクセスを防止するために、ユーザに個別の認証コードを与え、入力された認証コードが、予め登録されている認証コードと一致した場合にログインを許可するようになっている。

【0003】

しかしながら、上記のような認証システムは、認証コードを他人に知られると、許可されたユーザ以外の人でもアクセスできてしまうという問題点を有している。

【0004】

そのような問題点を解決するために、携帯電話に G P S 機能を持たせ、予めシステムにアクセスすることのできる位置範囲を登録しておき、アクセス時の携帯電話の位置が登録してある位置範囲外有的时候にはアクセスを拒否することで、不正なアクセスを防止するものがある（例えば特許文献 1 参照）。

【 0 0 0 5 】

また、携帯情報端末の使用行動範囲を記憶媒体に記憶しておき、G P S 制御モジュールから読み出した携帯情報端末の現在位置が、予め登録されている使用行動範囲内でないときには、ファイルの削除処理を実行することで携帯情報端末に記憶されているデータの漏洩を防止するものもある（例えば、特許文献 2 参照）。

【 0 0 0 6 】

【特許文献 1】

特開 2 0 0 2 - 3 2 7 5 6 2 号公報（図 5、段落 0 0 2 4 及び 0 0 2 5）

【特許文献 2】

特開 2 0 0 3 - 1 8 6 5 2 号公報（図 3、段落 0 0 1 5）

【 0 0 0 7 】

【発明が解決しようとする課題】

会社、公共機関、図書館等においては、そのエリアの中では自由に閲覧可能でも、外部への持ち出しが禁止された電子文書が存在する。今後、会社、公共機関における文書の電子化が進むにつれ、外部への持ち出しを禁止する電子文書が増加することが予想される。

【 0 0 0 8 】

また従来の技術では、携帯電話あるいは携帯情報端末自体が、所定の位置範囲外に持ち出された場合の不正なアクセス、あるいはデータの不正な利用を防止することはできるが、許可された位置範囲内であれば電子文書をコピーし、あるいはオリジナルの電子文書を許可された位置範囲外に持ち出すことが可能である。

【 0 0 0 9 】

本発明の課題は、指定した場所以外ではファイルを開くことができないようにすることである。

【0010】**【課題を解決するための手段】**

本発明は、ファイルのセキュリティ管理プログラムにおいて、コンピュータに、ファイルを開くことのできる位置を指定する位置情報をキーとして前記ファイルを暗号化する暗号化手段と、前記位置情報をキーとして暗号化されたファイルを保存する保存手段と、位置検出手段により検出される位置情報をキーとしてファイルを復号する復号化手段と、前記復号化手段により復号されたファイルを表示する表示手段として機能させる。

【0011】

この発明によれば、ファイルの保存時に指定された位置では自由にファイルを開くことができるが、それ以外の位置ではファイルを開くことができない。従って、ファイルを開くことができる場所でファイルがコピーされ、そのファイルが外部に持ち出された場合、あるいはファイルが格納されている携帯型の情報処理装置が指定された位置以外の場所に持ち出された場合でも、指定された場所以外の場所ではファイルを開くことができないので、ファイルが不正に利用されるのを防止できる。

【0012】

上記の発明において、前記暗号化手段は更に、ファイルを復号することが可能な位置情報の選択時に予め登録してある複数箇所の中から選択することができるようにする。

【0013】

このように構成することで、ファイルを保存するときに、予め登録してある複数箇所の中から任意の位置を指定することで、ファイルを開くことのできる位置を指定することができる。

【0014】

上記の発明において、前記暗号化手段は更に、暗号化のキーとして用いる位置情報のデータ長を変化させることで前記ファイルを開くことのできる範囲を限定する。

【0015】

このように構成することで、例えば、位置情報の何桁目以下を切り捨てるかによりファイルを開くことのできる位置範囲を任意に制限できるので、セキュリティ強度をユーザが任意に設定できる。

【0016】

図1 (A) 及び (B) は、本発明のファイルのセキュリティ管理装置の原理説明図である。

本発明のファイルのセキュリティ管理装置は、ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化する暗号化手段1と、前記位置情報をキーとして暗号化されたファイルを保存する保存手段2と、位置検出手段3により検出される位置情報をキーとしてファイルを復号する復号化手段4と、前記復号化手段4により復号されたファイルを表示する表示手段5とを備える。

【0017】

この発明によれば、ファイルの保存時に指定された位置では自由にファイルを開くことができるが、それ以外の位置ではファイルを開くことができないのでファイルのセキュリティを高めることができる。

【0018】

本発明の他のファイルのセキュリティ管理装置は、ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化する暗号化手段1と、前記位置情報をキーとして暗号化されたファイルを保存する保存手段2とを備える。

【0019】

この発明によれば、ファイルの保存時に指定された位置では自由にファイルを開くことができるが、それ以外の位置ではファイルを開くことができないのでファイルのセキュリティを高めることができる。

【0020】

【発明の実施の形態】

以下、本発明の実施の形態のファイルのセキュリティ管理方法を図面を参照しながら説明する。以下に述べる実施の形態は、ファイルのセキュリティ管理方法

に基づくセキュリティ管理プログラムを、文書作成用のアプリケーションプログラムに組み込んだ場合の例を示している。

【0021】

図1は、実施の形態のファイルのセキュリティ管理プログラムが実装された情報処理装置（セキュリティ管理装置）11の機能の説明図である。情報処理装置は、例えばパーソナルコンピュータにより実現される。

【0022】

GPS（Global Positioning System）装置（位置検出手段）12は、複数のGPS衛星からの電波を受信して現在位置の緯度及び経度データからなる位置情報を算出する。

【0023】

フィルタ部13は、位置情報にフィルタをかけて所定のデータ長の位置情報に変換し暗号化モジュール（暗号化手段）14に出力する。データの暗号化レベル、つまりファイルを開くことのできる位置の範囲をどの程度に設定するかはユーザにより指定されるので、フィルタ部13は、ユーザにより指定された暗号化レベルに対応するフィルタ処理を位置情報に対して行い、対応するデータ長を有する位置情報を暗号化の為のキーとして出力する。

【0024】

暗号化モジュール14は、入力ファイル（文書データ）を、フィルタ部13から出力される位置情報をキーとして暗号化する。

保存部15は、暗号化されたファイルのデータの先頭のヘッダに暗号化のレベルを示すデータを格納し、さらに、暗号化したデータから作成したダイジェストをフッタに格納し、それらのデータを1つのファイルとして出力する。暗号化されたファイルはハードディスク等の外部記憶装置に保存される。

【0025】

図3は、ファイルのセキュリティ管理プログラムを文書作成のアプリケーションに組み込んだ場合のツールバーの一例を示す図である。

表示画面の上部に表示されるツールバーのファイルの項目の下位階層のメニューには、従来からある「上書き保存」と「名前付けて保存」の選択肢の他に、フ

ファイルを開くことのできる場所として現在位置を指定する「この場所を指定して保存」と、ファイルを開くことのできる場所の緯度経度を指定して保存する「緯度経度を指定して保存」の2つの選択肢が追加されている。

【0026】

例えば、「緯度経度を指定して保存」を選択した場合には、保存時にユーザが緯度経度を指定し、あるいはユーザが予め指定した場所を、ファイルを開くことのできる場所としてファイルに設定することができる。ファイルの開くことのできる場所をファイルに設定する方法としては、ファイルを開くことのできる場所の位置情報をキーとしてデータを暗号化して保存する。これによりファイルを開く場合には、暗号化に使用された位置情報をキーとして復号する必要があるので、指定した場所以外ではファイルを開くことができなくなる。

【0027】

図4は、本発明の第1の実施の形態のデータを暗号化して保存する場合の保存処理のフローチャートである。以下に述べる処理は、情報処理装置11のCPUにより実行され、処理結果のデータは、メモリまたはハードディスク等に保存される。

【0028】

文書データ等を保存する場合に、暗号化保存が選択されたときには、CPUは、GPS装置12からGPS情報を取得する(図4, S11)。

次に、暗号化する際のセキュリティレベルがユーザにより指定されたなら、セキュリティレベルに対応するフィルタを指定する(図4, S12)。

【0029】

次に、暗号化して保存するデータを取得する(図4, S13)。そして、セキュリティレベルに対応したフィルタにより指定されるGPS情報の上位の所定桁数分の緯度経度データをキーとしてデータを暗号化する(図4, S14)。

【0030】

ここで、セキュリティレベルとは、緯度経度データの度、分、秒のデータの内の何桁目までのデータを暗号化のキーとして使用するかを定めるためのデータである。

【0031】

第1の実施の形態においては、図5に示すように、セキュリティレベルとフィルタの値とを対応づけたフィルタテーブル21を設けてあり、ユーザがファイルを保存するときにセキュリティレベル（ファイルを開くことのできる位置範囲）を指定することで、緯度経度データの内の上位何桁目のデータまでを暗号化のキーとして使用するかを決めている。

【0032】

例えば、セキュリティレベル4が選択された場合には、図5に示すフィルタテーブル21からフィルタ値として「111.10.00.00」が選択され、その値とGPS装置12から出力される経度データ、例えば東経134度33分19秒10（「134.33.19.10」）とが乗算される。この演算によりフィルタの値が「1」の桁に対応する経度データはそのまま出力され、フィルタの値が「0」の桁に対応する経度データは「0」となり、「134.30.00.00」が暗号化のためのキーとして得られる。

【0033】

セキュリティレベルとは、緯度経度データの上位何桁までを有効なデータとして利用するかということであり、セキュリティレベルを変えることで、暗号化したデータを復号できる位置範囲を任意に設定することができる。

【0034】

図5のフィルタテーブル21のセキュリティレベル0は、暗号化しない場合に該当し、セキュリティレベル1は、暗号化の鍵長が最も短い場合であり、最も広い範囲でファイルを開くことができる。セキュリティレベル9は、経度または緯度データの全ての桁を暗号化の鍵として使用する場合であり、最もセキュリティ強度を高くできる。

【0035】

図6は、セキュリティレベルにより定まる位置範囲を示す図である。例えば、A事業所が、東経139度43分45秒～55秒、北緯35度36分20秒～30秒の範囲（図6に斜線で示す範囲）に存在するときには、その範囲を指定できるようなフィルタの値を設定し、そのフィルタの値と、A事業所の緯度経度デー

タを乗算して得られる緯度経度データを暗号化キーとして用いる。これにより、A事業所内のどの位置においてもファイルを自由に開くことができ、それ以外の場所ではファイルを開くことができなくなる。すなわち、暗号化に用いるキーの長さを変えることで、緯度経度データに定まる任意の位置範囲をファイルを開くことのできる場所として指定することができる。

【0036】

図4に戻り、データの暗号化が終了したなら、ヘッダと、暗号化されたデータのダイジェストを生成する（図4，S15）。

次に、セキュリティレベルを示すデータを格納したヘッダと、位置情報により暗号化したデータと、ダイジェストを格納したフッターとを1つのファイルとして保存する（図4，S16）。

【0037】

図7は、上記のデータの保存処理により作成される暗号化されたファイルのデータ構成を示す図である。

図7に示すように、暗号化されたデータの先頭にセキュリティレベル等を示すデータ等からなるヘッダが付加され、暗号化されたデータの後にそのデータのダイジェストからなるフッタが付加される。

【0038】

図8は、図7のヘッダの構成を示す図である。ヘッダには、ファイル識別ヘッダと、経度及び緯度のセキュリティレベルを指定する経度セキュリティレベルデータ及び緯度セキュリティレベルデータと、経度緯度データの秒以下のセキュリティレベルを指定するための経度セキュリティサブレベルデータ及び緯度セキュリティサブレベルデータと、データの暗号化方式を指定する暗号化方式データ（例えば、位置情報を利用した暗号化、あるいは公開鍵による暗号化等を指定するデータ）と、暗号化した日時のデータと、データを保存した所有者データを示す所有者データ1，2とが設定される。

【0039】

ヘッダの緯度経度のセキュリティレベル及びセキュリティサブレベルは、ファイルを開くときに、GPS位置情報から復号のためのキーを作成する為に使用さ

れる。

【 0 0 4 0 】

図 9 は、次にファイルを開くことのできる場所として現在の場所を指定して保存する場合の処理のフローチャートである。

最初に、GPS 装置 1 2 から GPS 情報を取得する（図 9，S 2 1）。次に、現在位置の GPS 情報にハッシュ演算を行って得られるデータをキーとして文書データを暗号化する（図 9，S 2 2）。次に、暗号化したデータにヘッダ及びフッタを付加して記憶装置に保存する（図 9，S 2 3）。

【 0 0 4 1 】

図 1 0 は、ファイルを開くことのできる場所の緯度経度を指定して保存する場合の処理を示すフローチャートである。

ツールバーから「場所を指定して保存」が選択された場合には、予め設定してある場所の位置情報、あるいは、そのときユーザが指定した位置情報を取得する（図 1 0，S 3 1）。

【 0 0 4 2 】

次に、取得した位置情報にハッシュ演算を施して得られるデータをキーとしてデータを暗号化する（図 1 0，S 3 2）。

次に、暗号化したデータにヘッダとフッタを付加して記憶装置に保存する（図 1 0，S 3 3）。

【 0 0 4 3 】

図 1 1 は、「緯度経度を指定して保存」する場合の場所を指定する設定画面の表示例と、そのとき暗号化のキーとして用いられる緯度経度データを示す図である。

【 0 0 4 4 】

図 1 1 の例は、会社の各事業部名とそれぞれの場所の緯度経度データを対応づけたテーブルを予め作成しておいて、ユーザが事業所名を指定してファイルを保存すると、事業所のある位置の緯度経度データがテーブルから読み出され、その緯度経度データをキーとしてファイルが暗号化される。

【 0 0 4 5 】

この場合、事業所名を指定してファイルを暗号化して保存することで、該当する事業所内では自由にファイルを開くことができ、それ以外の場所ではファイルを開けなくすることができ、簡単な保存操作でファイルのセキュリティを高めることができる。

【0046】

次に、図12は、ファイルを開く場合の処理のフローチャートである。

最初に、ファイルのヘッダに暗号化のセキュリティレベルを示すデータが格納されているか否かを調べ、位置情報により暗号化されたファイルか否かを判断する(図12, S41)。

【0047】

ヘッダに暗号化のセキュリティレベルを示すデータが格納されているときには(S41, YES)、ステップS42に進み、内蔵されているGPS装置12、あるいは外付けのGPS装置12からGPS情報を取得する。

【0048】

次に、ヘッダから読み取ったセキュリティレベルに基づいてGPS情報にフィルタをかける(図12, S43)。

次に、フィルタをかけたGPS情報をキーとして暗号化されたデータを復号する(図12, S44)。そして、復号したデータを読み出して表示する(図12, S45)。

【0049】

次に、図13は、位置情報により暗号化されたファイルを開く場合の他の処理のフローチャートである。

最初に、GPS装置12から現在位置のGPS情報(緯度経度データ)を取得する(図13, S51)。次に、現在位置の緯度経度データに対して予め決められているハッシュ演算を施したデータをキーとしてファイルを復号する(図13, S52)。そして、復号したデータを読み出して表示する(図13, S53)。

【0050】

上述した第1の実施の形態によれば、ファイルを開くことのできる位置として

指定された位置（位置情報により定まる範囲を含む）において、ファイルを開く操作を行った場合には、その位置の位置情報によりファイルを復号してファイルの内容を表示させることができる。ファイルを開いた位置が、指定された位置と異なる場合には、その位置の位置情報ではファイルを復号することができないので意味のあるデータは表示されない。

【0051】

従って、仮にファイルを開くことのできる場所で、ファイルがコピーされて外部に持ち出されても、指定した場所以外では開くことができないのでファイルの不正な使用を防止できる。

【0052】

次に、図14は、本発明の第2の実施の形態のデータの送信・保存処理のフローチャートである。この第2の実施の形態は、データを位置情報をキーとして暗号化し、さらに位置情報により暗号化したデータを受信者の公開鍵により暗号化して送信・保存する例である。

【0053】

ファイルの送信または保存が指定されると、情報処理装置11のCPUは、GPS装置12からGPS位置情報を取得する（図14，S61）。

次に、暗号化レベル（セキュリティレベル）を元に位置情報にフィルタをかける（図14，S62）。

【0054】

次に、フィルタをかけた位置情報をキーとしてデータを暗号化する（図14，S63）。

次に、暗号化したデータのダイジェストを作成する（図14，S64）。ここで、ダイジェストは、暗号化したデータに対して所定のハッシュ演算を行った結果のデータを指す。

【0055】

次に、位置情報により暗号化したデータと、暗号化レベルを示す情報等からなるヘッダと、ダイジェストからなるフッタとを、メッセージの受信者の公開鍵で暗号化する（図14，S65）。

【0056】

次に、受信者の公開鍵で暗号化した暗号文（公開鍵で暗号化された、GPS暗号ヘッダ部とデータとGPS暗号フッター部とかなるデータ）に対して所定のハッシュ演算を行いダイジェストを作成する（図14，S66）。

【0057】

次に、受信者の公開鍵で暗号化した暗号文に公開鍵暗号ヘッダ部を付加し、作成したダイジェストを公開鍵フッター部に格納して送信または保存する（図14，S67）。

【0058】

図15は、上記のデータの送信・保存処理により作成されるデータの構成を示す図である。

図15に示すように、送信されるデータは、公開鍵暗号ヘッダ部と、公開鍵で暗号化された暗号文と、ダイジェストが格納される公開鍵暗号フッター部とからなる。公開鍵で暗号化された暗号文は、暗号化レベルを示すデータ等が格納されたGPS暗号ヘッダ部と、GPS位置情報をキーとして暗号化されたデータと、ダイジェストが格納されたGPS暗号フッターとで構成されている。

【0059】

次に、図16は、位置情報及び公開鍵により暗号化されたファイルを受信して、そのファイルを開く場合の処理のフローチャートである。

公開鍵で暗号化された暗号文に対して所定のハッシュ演算を行いダイジェストを作成し、そのダイジェストがフッター部に格納されているダイジェストと一致するか否かをチェックする（図16，S71）。

【0060】

ダイジェストが一致する場合には、暗号文を受信者の秘密鍵で復号する（図16，S72）。受信者の秘密鍵で復号すると、GPS暗号ヘッダ部と、GPS情報により暗号化された暗号文と、GPS暗号フッター部とが得られるので、GPS暗号ヘッダ部から暗号化レベルを示すデータを取得する（図16，S73）。

【0061】

次に、位置情報により暗号化された暗号文に対して所定のハッシュ演算を行い

ダイジェストを作成し、その作成したダイジェストがGPS暗号フッター部に格納されているダイジェストと一致するか否かをチェックする(図16, S74)

。

【0062】

ダイジェストが一致する場合には、GPS装置12から位置情報を取得する(図16, S75)。GPSヘッダ部から取得した暗号化レベルを元に位置情報にフィルタをかけ暗号化レベルに対応したデータ長の位置情報に変換する(図16, S76)。

【0063】

次に、フィルタをかけた位置情報をキーとして暗号文を復号する(図16, S77)。

復号したデータを取り出して表示装置に表示させる(図16, S78)。ステップS78の処理は、暗号化されたデータを復号する処理とは別の処理として実行しても良いし、その処理の一部として実行しても良い。

【0064】

上述した第2の実施の形態によれば、ファイルを開く位置を指定する位置情報をキーとしてファイルを暗号化し、さらにその暗号化したデータを公開鍵暗号方式で暗号化して送信することで、秘密鍵を有する受信者が特定の位置にいるときのみファイルを開くことができるので、ファイルのセキュリティをさらに高めることができる。この第2の実施の形態は、位置情報をキーとして暗号する方法と、既知の暗号化方法を用いた暗号化システムとを併用することができる。

【0065】

図17は、位置情報による暗号化を地図情報に適用した本発明の第3の実施の形態の説明図である。

この第3の実施の形態は、位置情報により暗号化された地図情報をCDROM、DVD等の記録媒体に記録してユーザに提供し、ユーザがその地図情報を位置情報をキーとして復号するものである。

【0066】

地図情報の提供者は、地図情報を地域を指定する位置情報をキーとして暗号し

て記録媒体 31 に記録して販売する。

地図情報が記録された記録媒体 31 を購入したユーザは、その記録媒体 31 をカーナビゲーションシステムの読み取り装置にセットする。ユーザの運転する車が、地図を利用できる有効範囲を走行しているときには、カーナビゲーションシステムに搭載されている GPS 装置が取得した位置情報をキーとして記録媒体 31 に記録されている地図情報を復号することで、地図情報をカーナビゲーションシステムの表示装置 32 に表示させることができる。

【0067】

他方、ユーザの車が有効範囲外を走行しているときには、GPS 装置が取得した位置情報を用いて地図情報を復号しようとしても、暗号化された地図情報を復号することができないので、表示装置 32 に地図情報を表示させることができない。

【0068】

上述した第 3 の実施の形態によれば、地図情報を提供する提供者側は、地図情報を位置情報をキーとして暗号化することで、許可された範囲の地図情報のみをユーザが利用できるようにユーザの利用を制限できる。ユーザ側では、地図情報を復号するための特別の入力操作を行うことなく必要な地図情報を表示させることができる。

【0069】

次に、図 18 は、本発明の第 4 の実施の形態の暗号化された地図データを開く処理のフローチャートである。

この第 4 の実施の形態は、カーナビゲーションシステムを販売する会社などが、地図データをアクセスキーと位置情報により暗号化してユーザに送信し、ユーザが位置情報とアクセスキーにより地図データを復号するものである。

【0070】

第 4 の実施の形態の地図データは、その地図データを復号することのできる地域を指定する位置情報により暗号化され、さらに、その暗号された地図データがユーザの利用権限を示すアクセスキーにより暗号化されている。

【0071】

先ず、無線、あるいは通信回線を介して受信した暗号化された地図データに所定のハッシュ演算を行ってダイジェストを作成し、そのダイジェストが、地図データに付加されているダイジェストと一致する否かをチェックする（図18，S81）。

【0072】

ダイジェストが一致した場合には、ユーザに付与されているアクセスキーで地図データを復号する（図18，S82）。

次に、復号したデータの先頭のGPS暗号のヘッダ部から暗号レベルを示すデータを取得する（図18，S83）。

【0073】

次に、アクセスキーにより復号したデータに所定のハッシュ演算を行いダイジェストを作成し、GPS暗号のフッターに付加されているダイジェストと比較してダイジェストのチェックを行う（図18，S84）。

【0074】

ダイジェストが一致した場合には、GPS装置から現在位置の位置情報を取得する（図18，S85）。さらに、ヘッダから取得した暗号化レベルを元に位置情報にフィルタをかける（図18，S86）。ステップS86の処理では、暗号化レベルに応じて位置情報の下位の何桁かのデータを切り捨てることで位置情報にフィルタをかけ、暗号化されたデータを復号できる位置範囲を限定している。

【0075】

次に、フィルタをかけた位置情報をキーにして地図データを復号する（図18，S87）。

そして、復号した地図データを読み出してカーナビゲーションシステムの表示装置に表示させる（図18，S88）。このステップS88の処理は、暗号化された地図データを復号する処理に含めても良いし、復号化処理とは別の処理として実行しても良い。

【0076】

次に、図19は、複数の地域の地図情報を暗号化して1枚の記録媒体（CDROM、DVDなど）に記録する場合の説明図である。

図19の例は、記録媒体31に複数の地域の地図情報を、アクセスキーと地域を指定する位置情報をキーとして暗号化して記録しておき、地図情報を購入したユーザにそのユーザが利用できる地域の利用権が設定されたアクセスキーを付与するものである。

【0077】

地図情報が記録された記録媒体31を購入したユーザは、記録媒体31をカーナビゲーションシステムの読み取り装置にセットし、さらに地図情報の販売者から与えられたアクセスキーを入力する。カーナビゲーションシステムは、アクセスキーとGPS装置が取得する現在位置情報をキーとして記録媒体31に記録されている地図情報を復号する。

【0078】

例えば、ユーザが南関東の地図情報を購入している場合には、ユーザの車が南関東のエリアを走行しているときには、南関東の地図情報の利用権が設定されているアクセスキーとGPS装置により取得される位置情報とをキーとして地図情報を復号することで、南関東の地図情報を表示装置32に表示させることができる。この場合、他の地域の地図情報はそのアクセスキーでは利用できないので復号することができない。

【0079】

また、ユーザが東日本の地図情報を購入した場合には、東日本の地図情報の利用権が設定されているアクセスキーとGPS装置により取得される位置情報とをキーとして地図情報を復号することで、東日本の全ての地域の地図情報をカーナビゲーションシステムの表示装置に表示させることができる。

【0080】

図19の例では、1つの記録媒体31に日本の全ての地域の地図情報をアクセスキーとそれぞれの地域の位置情報をキーとして暗号化して記録しておくことで、ユーザが利用できる地図情報の範囲を任意に設定できる。また、地図情報の利用範囲が異なる複数のユーザに提供する記録媒体31を共通化できる。これにより、記録媒体31の作成工数を少なくできる。さらに、ユーザは、複数の地域の地図情報を必要とする場合でも、複数の地域を利用できるアクセスキーを入手す

ることで、1枚の記録媒体で複数の地域の地図情報を利用することができる。

【0081】

次に、図20は、リムーバブルメディアにアクセスキーを保存した場合の説明図である。

図20に示す例の地図情報の復号手順は、基本的には図19の例と同じである。異なる点は、アクセスキーをリムーバブルメディア33に保存しておくことで、ユーザが地図情報を利用するときに、そのリムーバブルメディア33をカーナビゲーションシステムのリムーバブルメディアの読み取り装置に挿入することで、ユーザが利用権限を持つ地域の地図情報を復号することができる点である。

【0082】

図20に示す例では、図19に示す暗号化方法の効果に加え、ユーザはリムーバブルメディアを読み取り装置に挿入するだけで必要な地図情報を表示させることができるのでアクセスキーを覚えておく必要がなくなる。また、地図情報の提供者側にとっては、リムーバブルメディアを使用しないと地図情報を復号できないので、アクセスキーがコピーされて不正に地図情報が利用されるのを防止できる。

【0083】

次に、図21は、本発明の第5の実施の形態のライセンス保護ファイルの実行処理のフローチャートである。

この第5の実施の形態は、ソフトウェアの実行に位置情報による暗号化を適用した例を示している。ソフトウェアを通信回線を介して提供する事業者は、ユーザがソフトウェアのダウンロードのライセンスを購入する際に、ユーザにコンピュータが設置されている場所を入力してもらい、その場所を特定する位置情報をライセン情報として発行する。この際オフラインでライセンス情報を発行してもかまわない。

【0084】

ユーザは、ソフトウェアをロード・実行もしくはダウンロードするためのライセンス情報を取得したなら、サーバをアクセスしてソフトウェアのダウンロードの手続きを開始する。

【0085】

最初に、コンピュータに接続されているGPS装置から位置情報を取得する（図21，S91）。

次に、GPS装置から取得した位置情報とライセンス情報を比較して両者が一致するか否かを判定する（図21，S92）。

【0086】

位置情報が一致する場合には、ステップS93に進み、サーバからソフトウェアプログラムをダウンロードし、ライセンス情報により復号して元のプログラムを再生する。なお、サーバからプログラムを送信する場合、プログラムをユーザ登録を行った位置情報により暗号化して送信する。ネットワーク上からダウンロードする方式でなくディスク上からメモリにロードする場合も同じ手法を用いることが可能である。したがってスタンドアロンのシステムでも本方式を応用可能である。

【0087】

GPS装置から取得した位置情報とライセンス情報が一致しない場合には、ソフトウェアをダウンロードせずに処理を終了する（図21，S94）。

上述した第5の実施の形態によれば、ソフトウェアのロード・実行もしくはダウンロードを、アクセスキーを取得するときに登録したコンピュータが設置されている場所でのみ行うことができ、アクセスキーを不正に入手してもプログラムをロード・実行もしくはダウンロードすることはできない。従って、プログラムの不正取得を防止し、ソフトウェアの保護をより強化することができる。また、プログラムを位置情報により暗号化することで、指定した位置以外ではそのプログラムを復号できないので、プログラムがコピーされても他の場所では使用できないようにできる。

【0088】

なお、ソフトウェアを購入したユーザに付与するライセンスキーをユーザのコンピュータが設置されている場所の位置情報により暗号化して発行するようにしても良い。

【0089】

このようにすることで、ライセンスキーを使用してプログラムをダウンロード

、あるいはプログラムをインストールするときに、登録した場所以外の場所ではライセンスキーを正しく復号できないので、同一のライセンスキーを複数の場所で使用することができなくなる。この場合、プログラム自体は位置情報により暗号化しなくとも良い。

【0090】

次に、図22は、実施の形態の情報処理装置11のハードウェア構成の一例を図22を参照して説明する。

CPU41は、データを位置情報により暗号化して保存する処理及び位置情報により暗号化されたデータを復号する処理等を実行する。GPS装置42は、複数の衛星からの電波を受信して現在位置の位置情報を算出する。

【0091】

外部記憶装置43にはCPU41により実行されるプログラムが格納されると共に、処理結果のデータ等が格納される。メモリ44は、演算に使用される各種のレジスタとして使用される。

【0092】

記録媒体駆動装置45は、CDROM、DVD、フレキシブルディスク、ICカード等の可搬記録媒体46の読み取り、あるいは書き込みを行う。

入力装置47は、キーボード等のデータを入力する装置である。出力装置48は表示装置などである。

【0093】

ネットワーク接続装置49は、LAN、インターネット等のネットワークに接続するための装置であり、この装置を介してネットワーク上の情報提供者のサーバからプログラムをダウンロードすることができる。なお、CPU41、メモリ44、外部記憶装置43等はバス50により接続されている。

【0094】

(付記1) ファイルのセキュリティ管理プログラムにおいて、
コンピュータに、ファイルを開くことのできる位置を指定する位置情報をキーとして前記ファイルを暗号化する暗号化手段と、前記位置情報をキーとして暗号化されたファイルを保存する保存手段と、位置検出手段により検出される位置情

報をキーとしてファイルを復号する復号化手段と、前記復号化手段により復号されたファイルを表示する表示手段として機能させるためのセキュリティ管理プログラム。

【0095】

(付記2) 付記1記載のファイルのセキュリティ管理プログラムであって、前記暗号化手段は更に、ファイルを復号することが可能な位置情報の選択時に予め登録してある複数箇所の中から選択する。

【0096】

(付記3) 付記1記載のファイルのセキュリティ管理プログラムであって、前記暗号化手段は更に、暗号化のキーとして用いる位置情報のデータ長を変化させることで前記ファイルを開くことのできる範囲を限定する。

【0097】

(付記4) ファイルのセキュリティ管理プログラムにおいて、利用できる位置を指定する位置情報をキーとしてデータを暗号化した暗号化済データを有し、コンピュータに、予めファイルを開くことのできる位置が指定された位置情報をキーとして保存しておき、位置検出手段により検出される位置情報に基づき、前記キーと合致するか否かを判定し、合致する場合は前記暗号化済データを復号する復号化手段と、前記復号化手段により復号されたデータを表示する表示手段として機能させるためのセキュリティ管理プログラム。

【0098】

(付記5) ファイルのセキュリティ管理装置において、ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化する暗号化手段と、前記位置情報をキーとして暗号化されたファイルを保存する保存手段と、位置検出手段により検出される位置情報をキーとしてファイルを復号する復号化手段と、前記復号化手段により復号されたファイルを表示する表示手段とを備えることを特徴とするセキュリティ管理装置。

【0099】

(付記6) コンピュータを、ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化する暗号化手段と、位置情報をキーとして暗

号化したファイルを記憶手段に保存する保存手段として機能させるファイルのセキュリティ管理プログラム。

【0 1 0 0】

(付記 7) コンピュータを、ファイルを開くときに、位置検出手段により検出される位置情報をキーとして暗号化されたファイルを復号する復号化手段と、復号されたファイルを表示させる表示手段として機能させるファイルのセキュリティ管理プログラム。

【0 1 0 1】

(付記 8) 暗号化手段が、データを利用することのできる位置を指定する位置情報によりデータを暗号化し、

保存手段が、前記暗号化されたデータを送信またはコンピュータ読み取り可能な記録媒体に保存するデータのセキュリティ管理方法。

【0 1 0 2】

(付記 9) 付記 8 記載のファイルのセキュリティ管理方法であって、暗号化のキーとして用いる位置情報のデータ長を変化させることでファイルを開くことのできる範囲を限定する。

【0 1 0 3】

(付記 1 0) 利用することのできる位置を指定する位置情報により暗号化された地図データを記録したコンピュータ読み取り可能な記録媒体。

(付記 1 1) 暗号化手段が、プログラムを利用することのできる位置を指定する位置情報によりプログラムを暗号化し、

保存手段が、前記暗号化されたプログラムを送信またはコンピュータ読み取り可能な記録媒体に記録するプログラムのセキュリティ管理方法。

【0 1 0 4】

(付記 1 2) 付記 1 1 記載のプログラムのセキュリティ管理方法であって、前記暗号化手段は、前記プログラムを前記位置情報とユーザに付与されるライセンスキーとにより暗号化する。

【0 1 0 5】

(付記 1 3) 使用することのできる位置を指定する位置情報により暗号化され

たプログラムを記録したコンピュータ読み取り可能な記録媒体。

(付記 14) ファイルを開くことのできる位置を指定する位置情報をキーとして前記ファイルを暗号化する暗号化手段と、暗号化されたファイルを保存する保存手段とを備えるファイルのセキュリティ管理装置。

【0106】

(付記 15) 位置検出手段により検出される位置情報をキーとしてファイルを復号する復号化手段と、前記復号化手段により復号されたファイルを表示させる表示手段とを備えるファイルのセキュリティ管理装置。

【0107】

(付記 16) 暗号化手段が、ファイルを開くことのできる位置を指定する位置情報をキーとしてファイルを暗号化し、保存手段が、前記位置情報をキーとして暗号化したファイルを保存し、復号化手段が、ファイルを開くときに、位置検出手段により検出される位置情報をキーとして前記ファイルを復号し、表示手段が、復号されたファイルを表示させるファイルのセキュリティ管理方法。

【0108】

上述した実施の形態は、本発明に係るセキュリティ管理プログラムを文書作成のアプリケーションのプラグインとして組み込んだ場合について説明したが、これに限らず、ファイル、あるいはデータを位置情報をキーとして暗号化して保存、あるいは送信する専用のプログラムとして実現してもよい。

【0109】

【発明の効果】

本発明によれば、保存時に指定された場所ではファイルを自由に開くことができるが、それ以外の場所ではファイルを復号して開くことができないので、ファイルのセキュリティを高めることができる。また、データを位置情報により暗号化して記録媒体に記録することで、ユーザがデータを利用できる場所を制限することができる。また、プログラムを位置情報により暗号化することでユーザがプログラムを使用できる場所を制限することができる。

【図面の簡単な説明】

【図 1】

図 1 (A)、(B) は、発明の原理説明図である。

【図 2】

実施の形態の情報処理装置の機能の説明図である。

【図 3】

アプリケーションのツールバーを示す図である。

【図 4】

第 1 の実施の形態のデータの保存処理のフローチャートである。

【図 5】

セキュリティレベルとフィルタと G P S 情報との関係を示す図である。

【図 6】

セキュリティレベルの説明図である。

【図 7】

暗号化されたファイルのデータ構成を示す図である。

【図 8】

ヘッダの構成を示す図である。

【図 9】

現在の場所を指定して保存する場合の処理を示すフローチャートである。

【図 1 0】

緯度経度を指定して保存する場合の処理を示すフローチャートである。

【図 1 1】

場所を指定して保存する場合の指定方法の説明図である。

【図 1 2】

ファイルを開く場合の処理のフローチャート (1) である。

【図 1 3】

ファイルを開く場合の処理のフローチャート (2) である。

【図 1 4】

第 2 の実施の形態のデータ送信・保存処理のフローチャートである。

【図 1 5】

暗号化されたデータの構成を示す図である。

【図 16】

ファイルを開く場合の処理のフローチャートである。

【図 17】

第3の実施の形態の説明図である。

【図 18】

第4の実施の形態の暗号化された地図データを開く処理のフローチャートである。

【図 19】

地図情報を記録媒体に記録した場合の説明図である。

【図 20】

リムーバブルメディアにアクセスキーを記録した場合の説明図である。

【図 21】

第5の実施の形態のライセンス保護ファイルの実行処理のフローチャートである。

【図 22】

情報処理装置の構成図である。

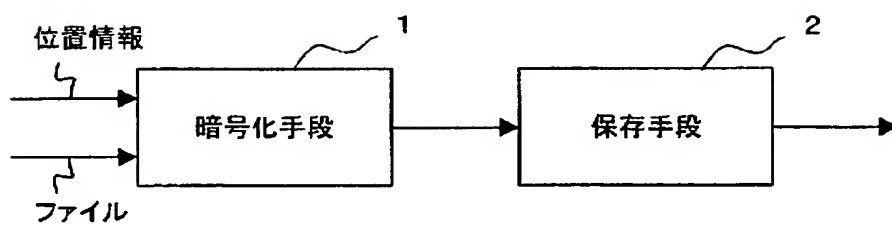
【符号の説明】

- 1 暗号化手段
- 2 保存手段
- 3 位置検出手段
- 4 復号化手段
- 5 表示手段
- 11 情報処理装置
- 12 GPS装置
- 13 フィルタ部
- 14 暗号化モジュール
- 15 保存部

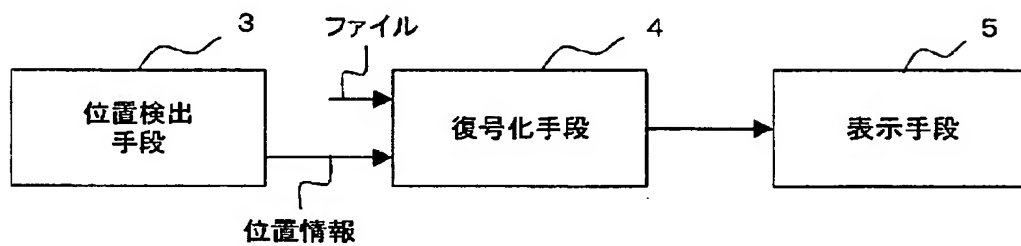
【書類名】 図面

【図 1】

発明の原理説明図



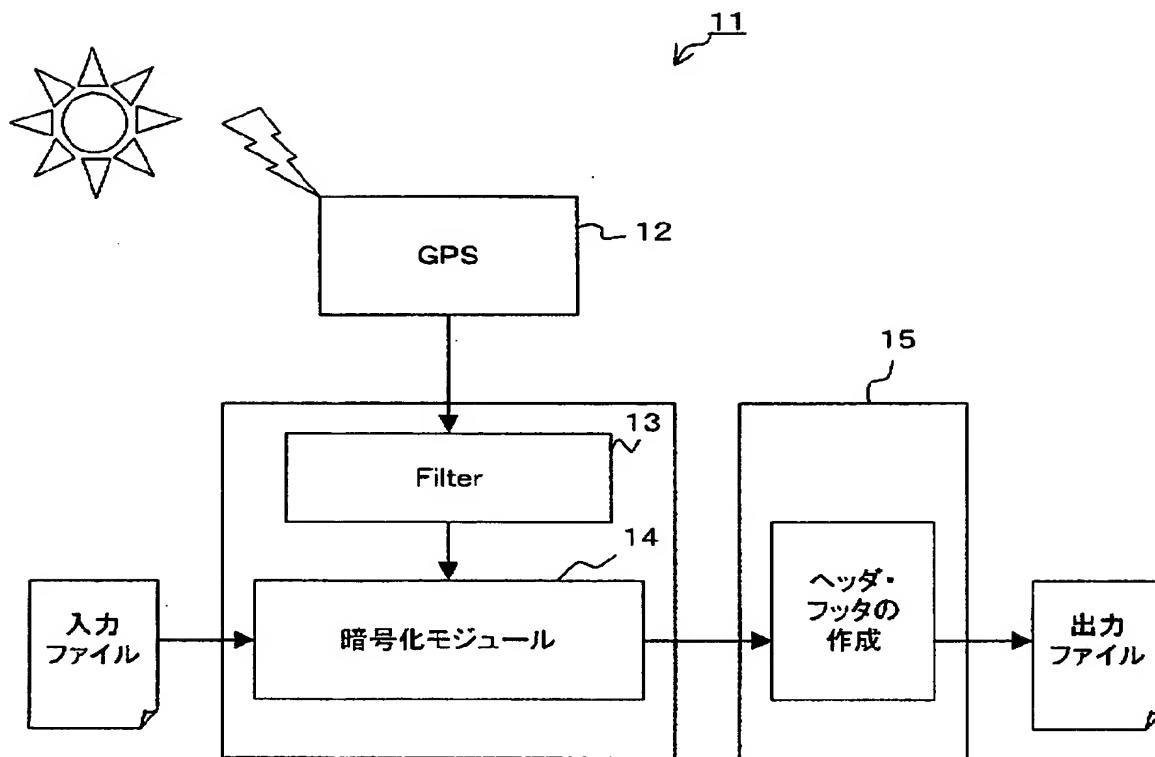
(A)



(B)

【図 2】

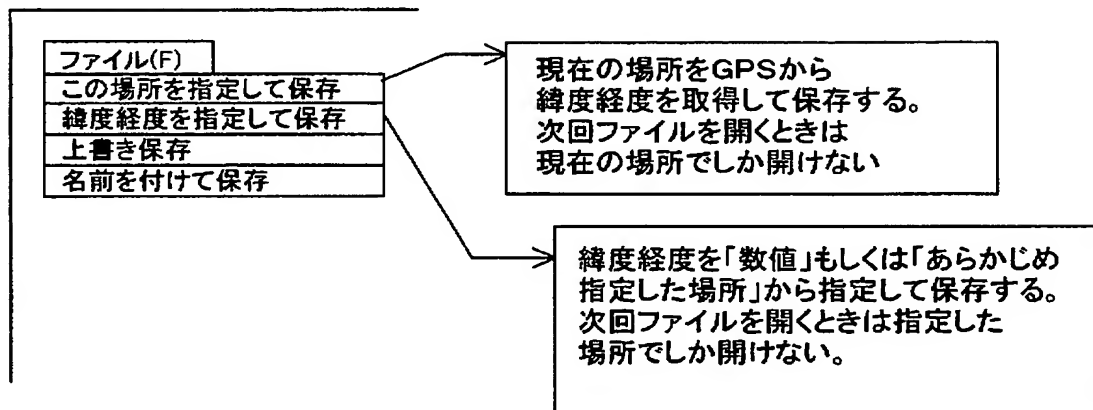
情報処理装置の機能の説明図



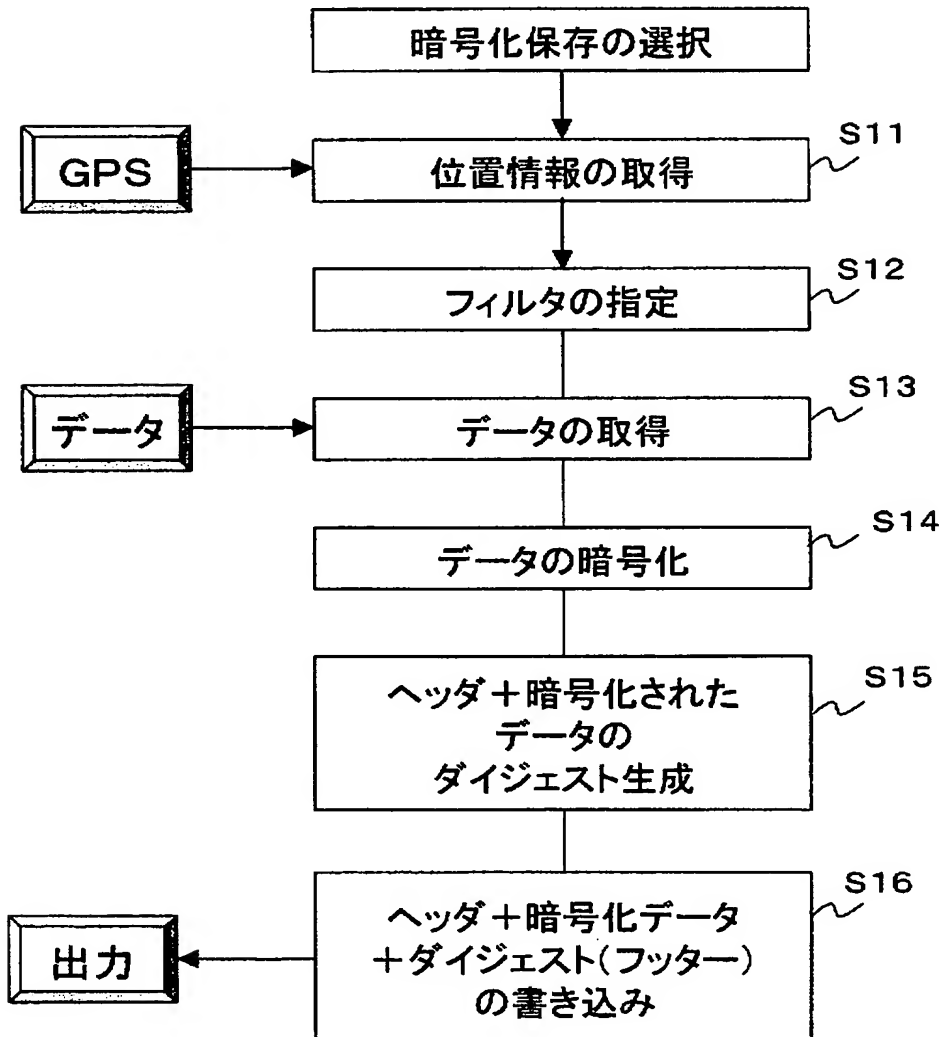
【図 3】

アプリケーションのツールバーを示す図

●アプリケーションのツールバー

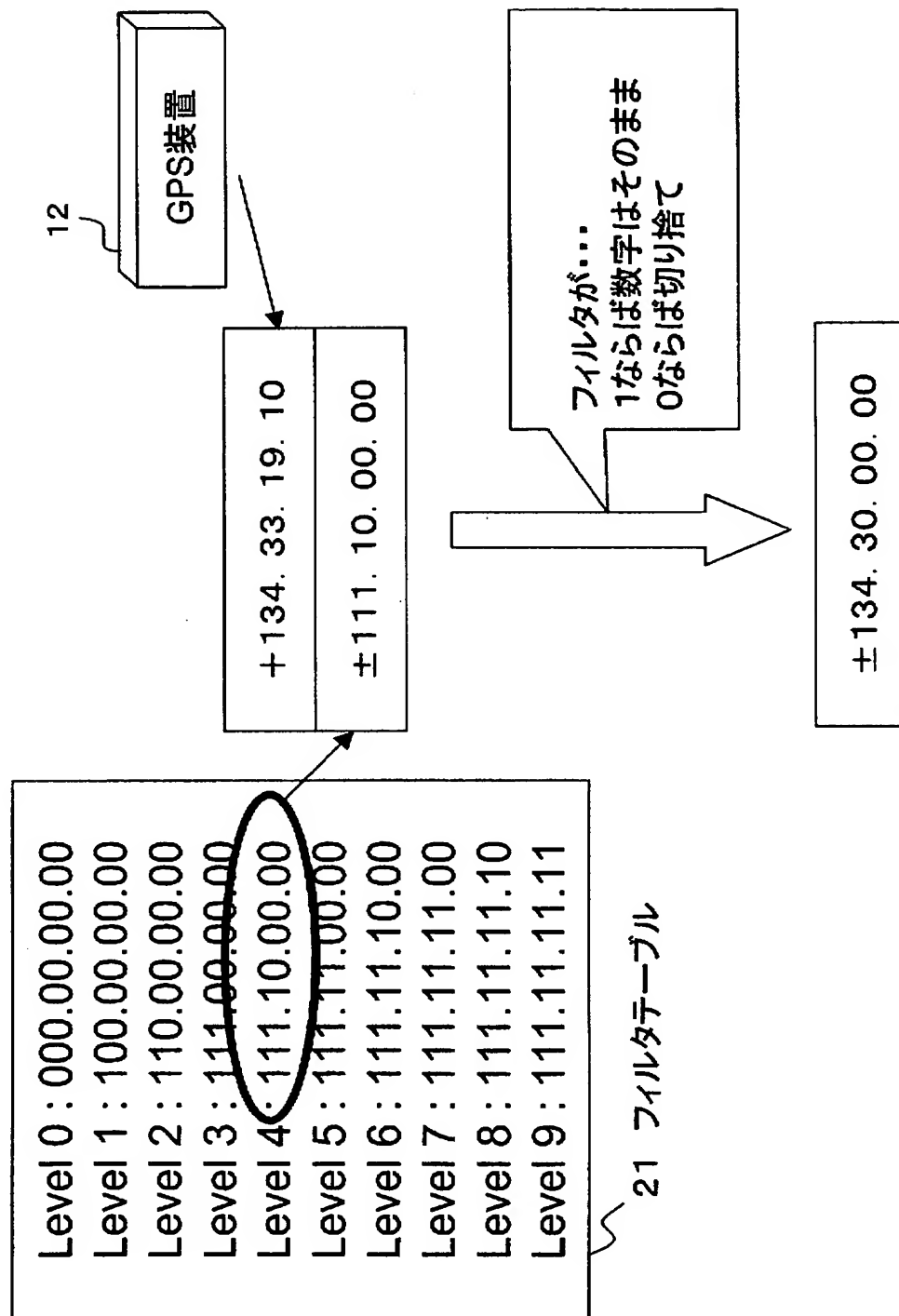


【図 4】

第1の実施の形態の
データの保存処理のフローチャート

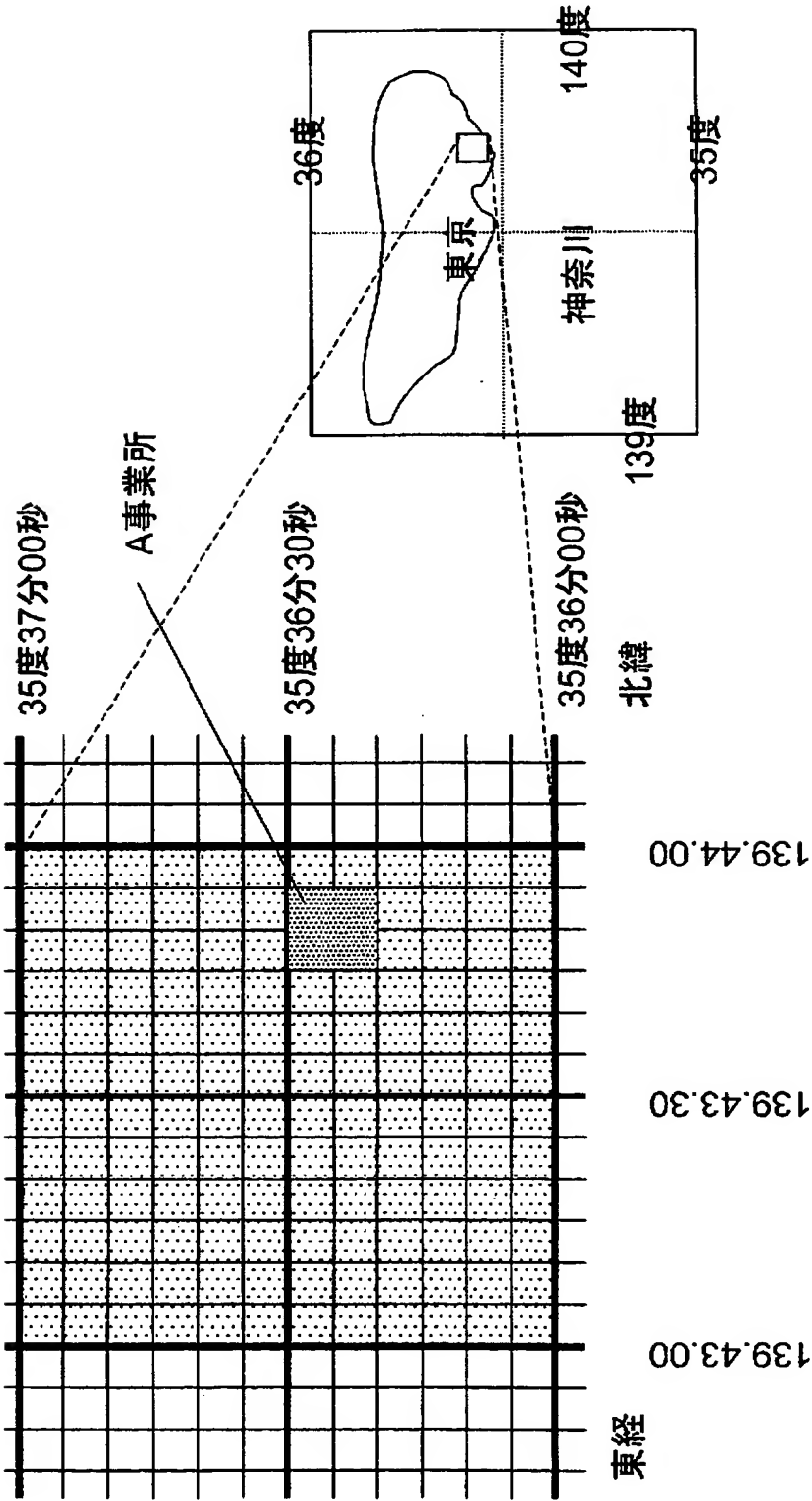
【図 5】

セキュリティレベルと
フィルタとGPS情報との関係を示す図



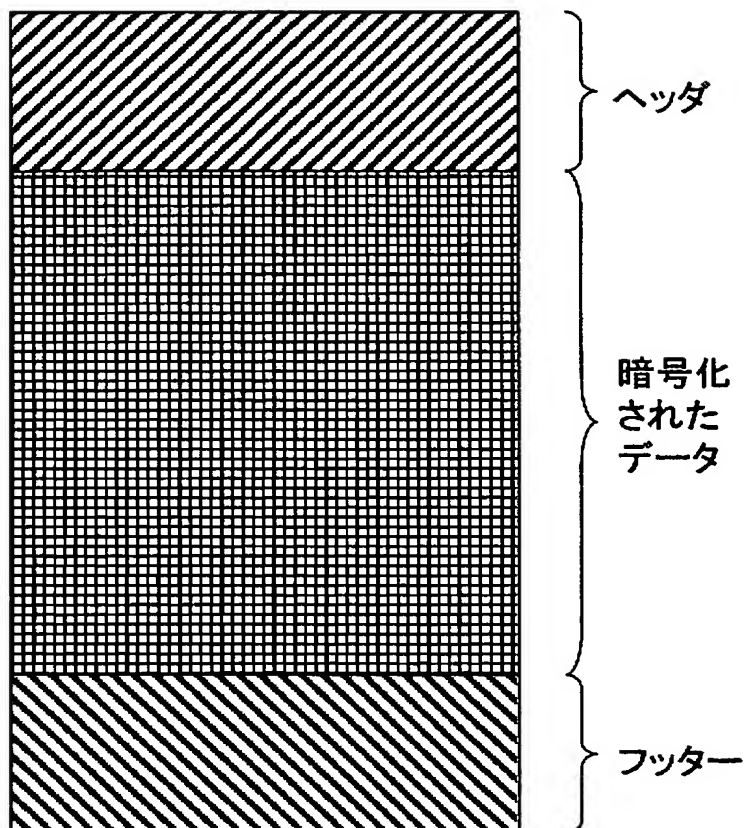
【図 6】

セキュリティレベルの説明図



【図 7】

暗号化されたファイルの
データ構成を示す図



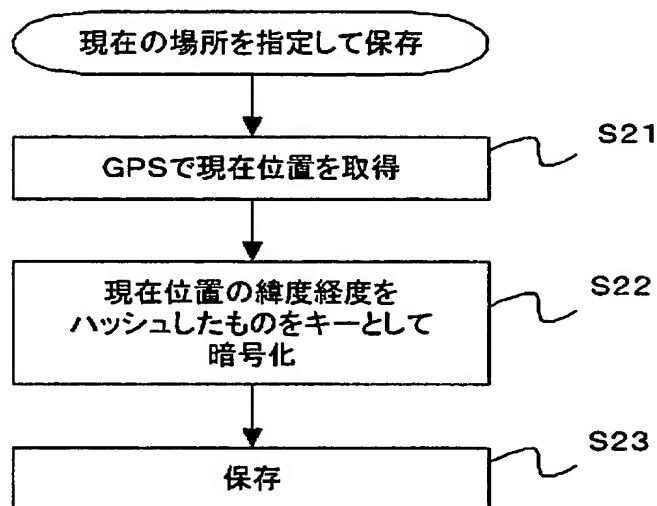
【図 8】

ヘッダの構成を示す図

ファイル識別ヘッダ		バージョン	予約領域
経度セキュリティレベル		経度セキュリティサブレベル	
緯度セキュリティレベル		緯度セキュリティサブレベル	
暗号化方式1	暗号化方式2	暗号化日時	
所有者データ1		所有者データ2	
拡張領域			

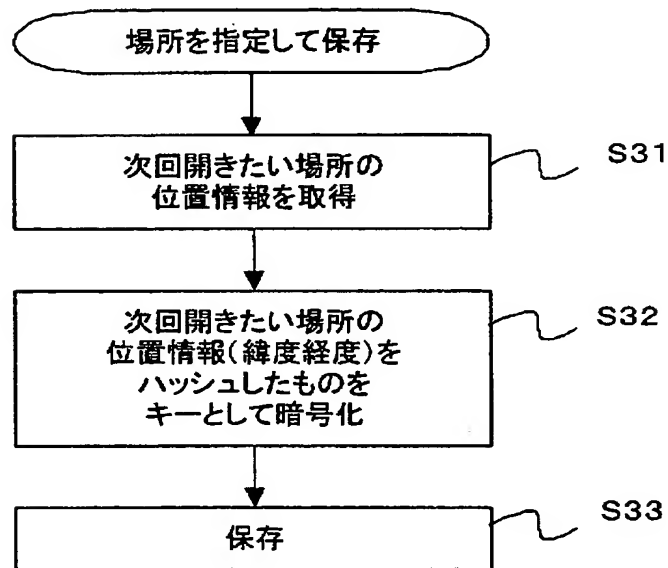
【図 9】

現在の場所を指定して
保存する場合の処理のフローチャート



【図 10】

緯度経度を指定して
保存する場合の処理のフローチャート



【図 1 1】

場所を指定して保存する場合の 指定方法の説明図

(設定画面例)

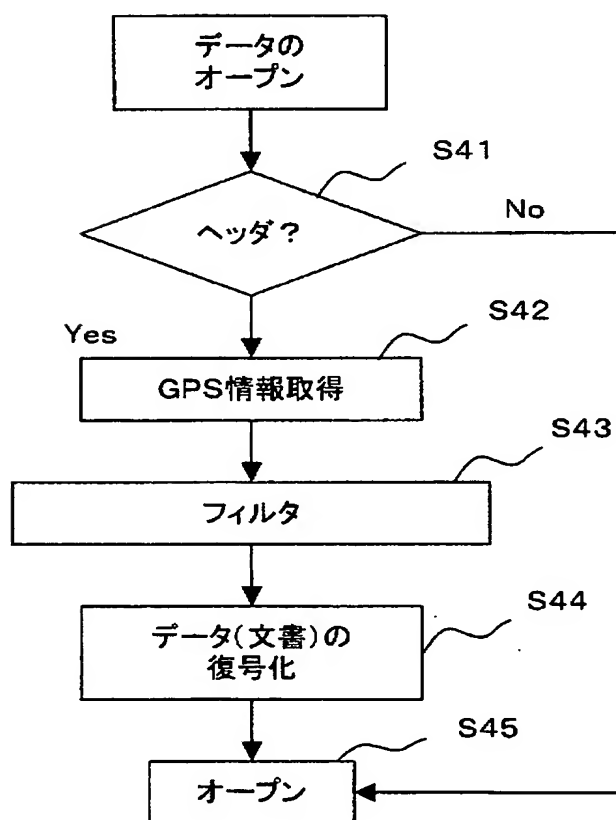
☐全事業所(社外秘)
☐本社 ☐恵比寿ビル ☐大井町ビル
☐蒲田シスラボ ☒幕張シスラボ

(書き込まれるデータ)

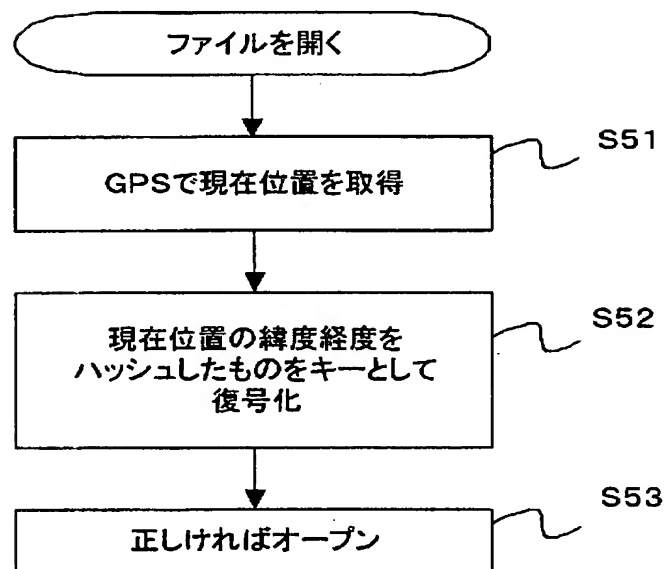
34-00-36N 13048-43E~33-41-23N 12958-58E

【図 12】

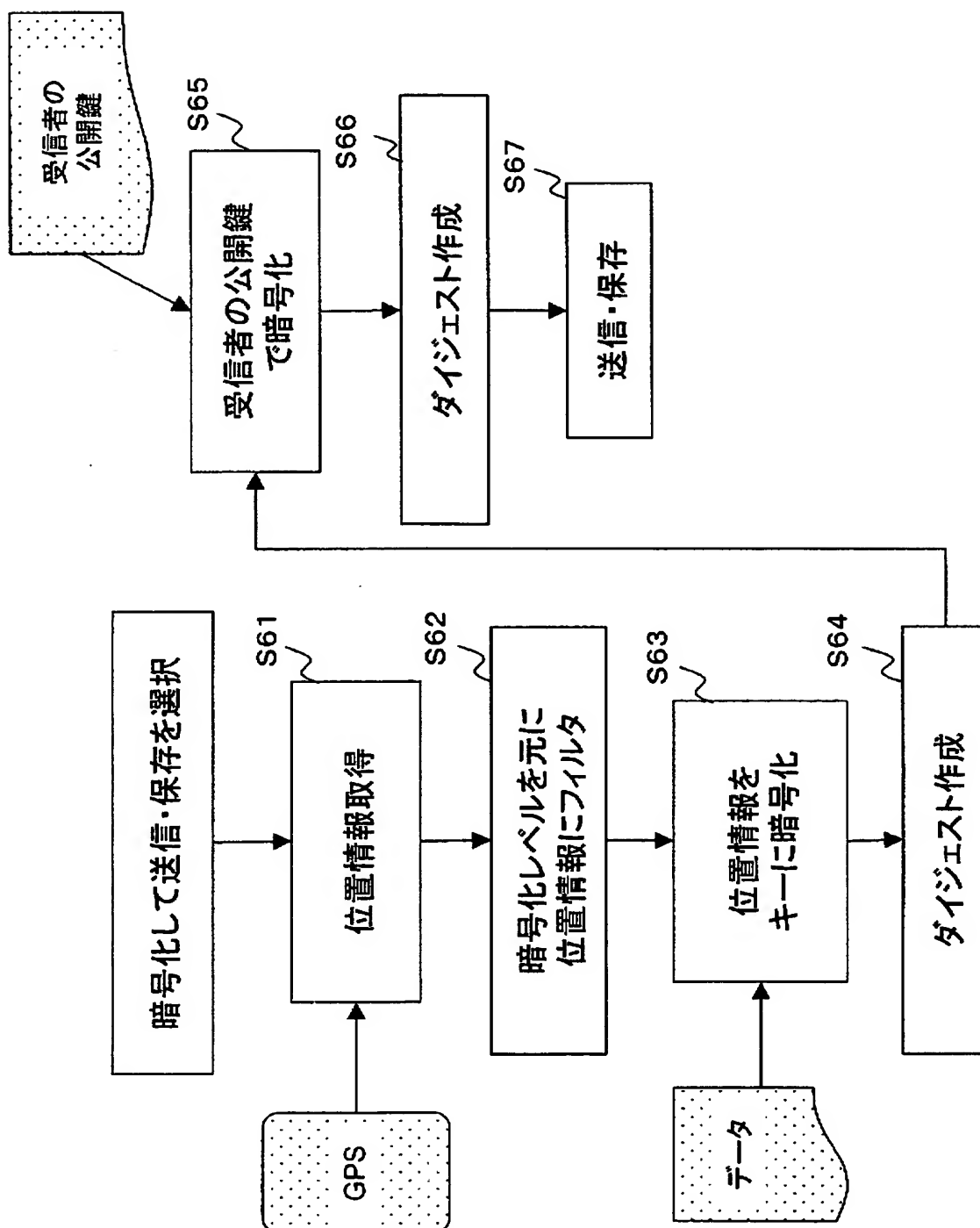
ファイルを開く場合の処理フローチャート(1)



【図 13】

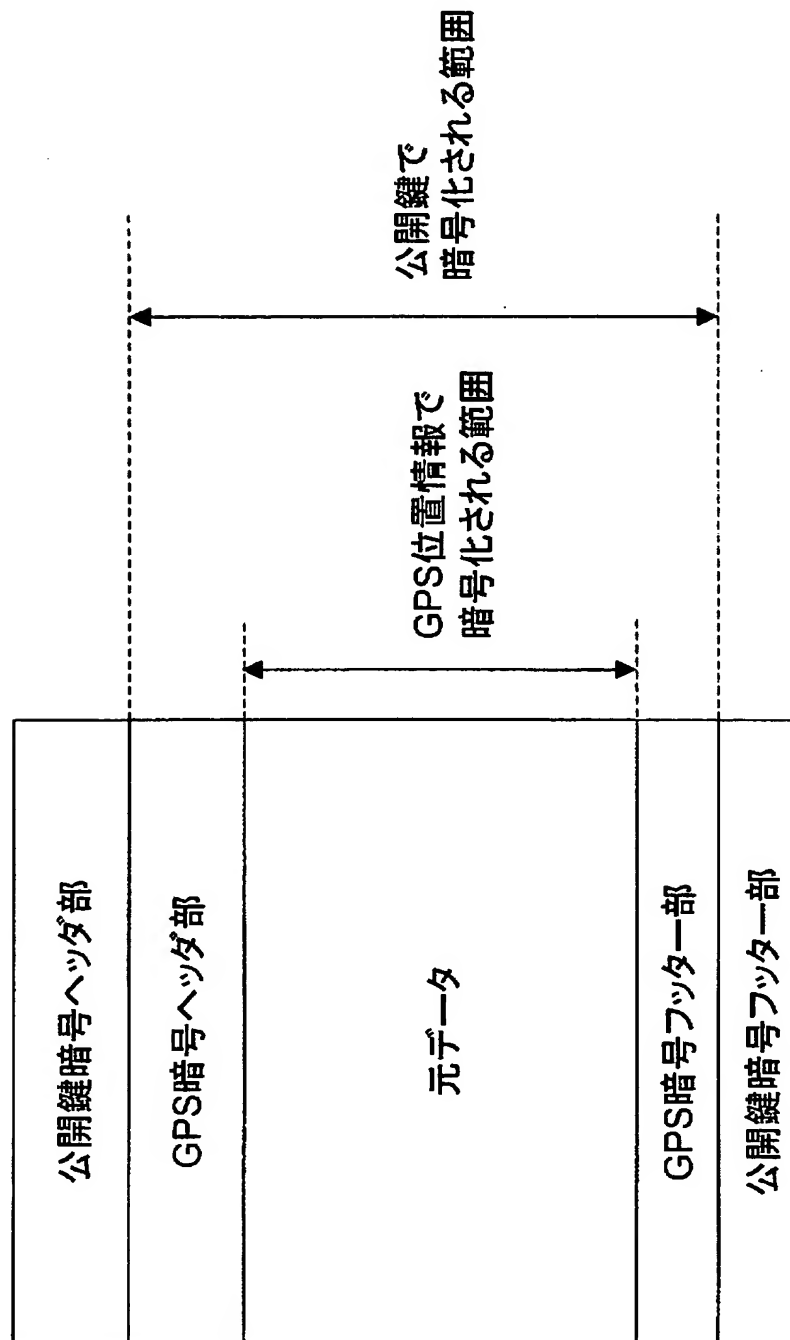
ファイルを開く場合の
処理のフローチャート(2)

【図 14】

第2の実施の形態の
データ送信・保存処理のフローチャート

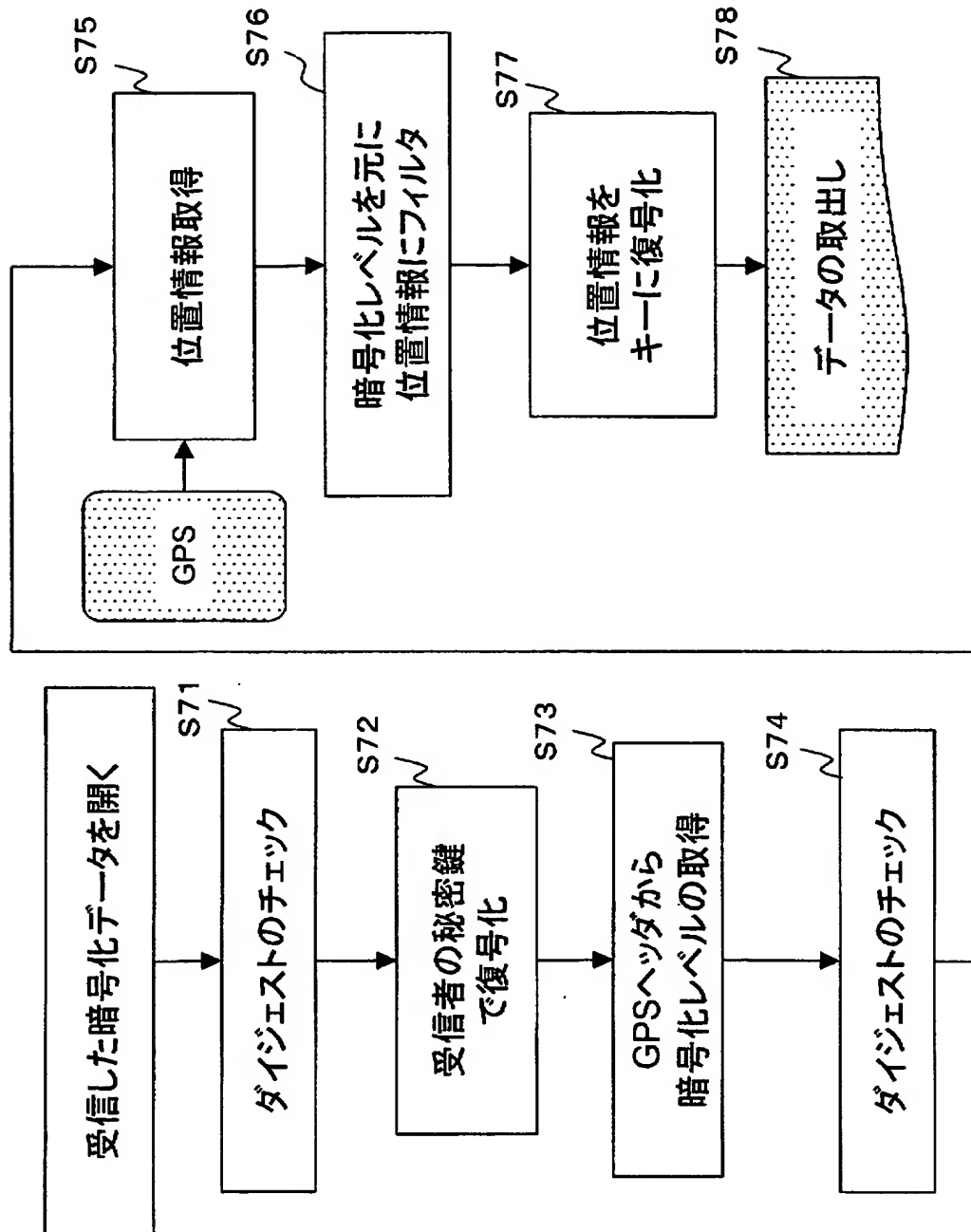
【図 15】

暗号化されたデータの構成を示す図



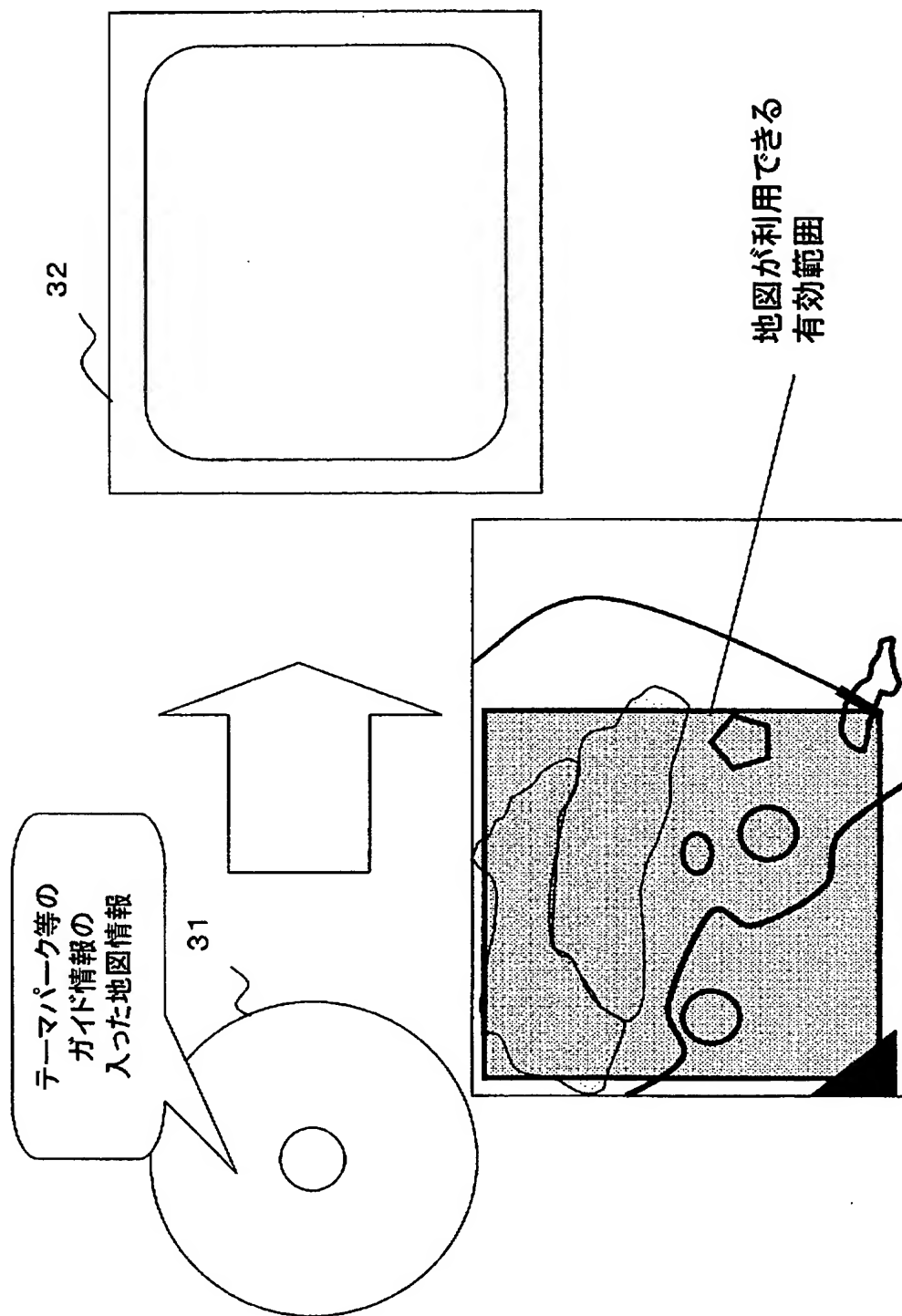
【図 16】

ファイルを開く場合の処理のフローチャート



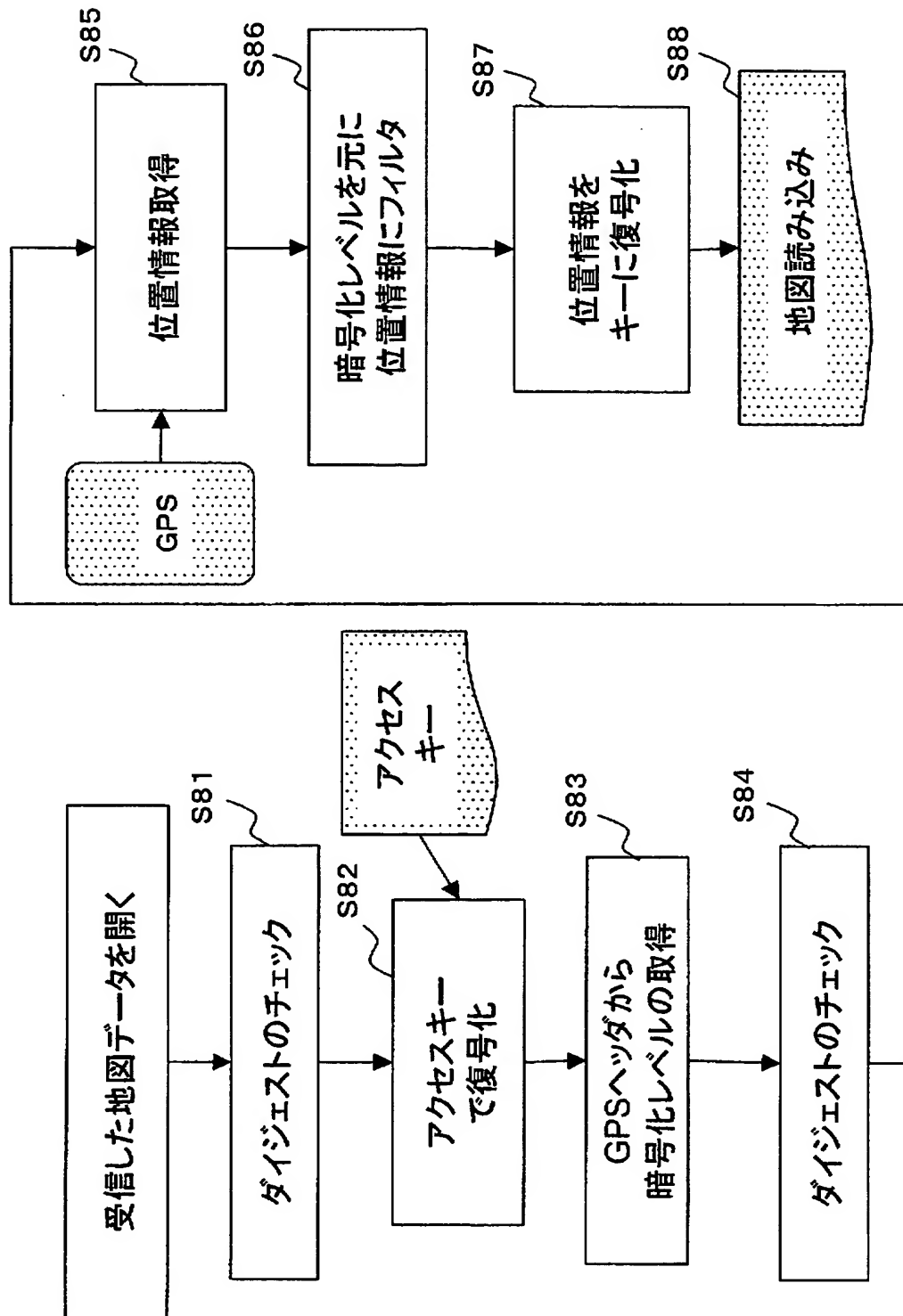
【図 17】

第3の実施の形態の説明図



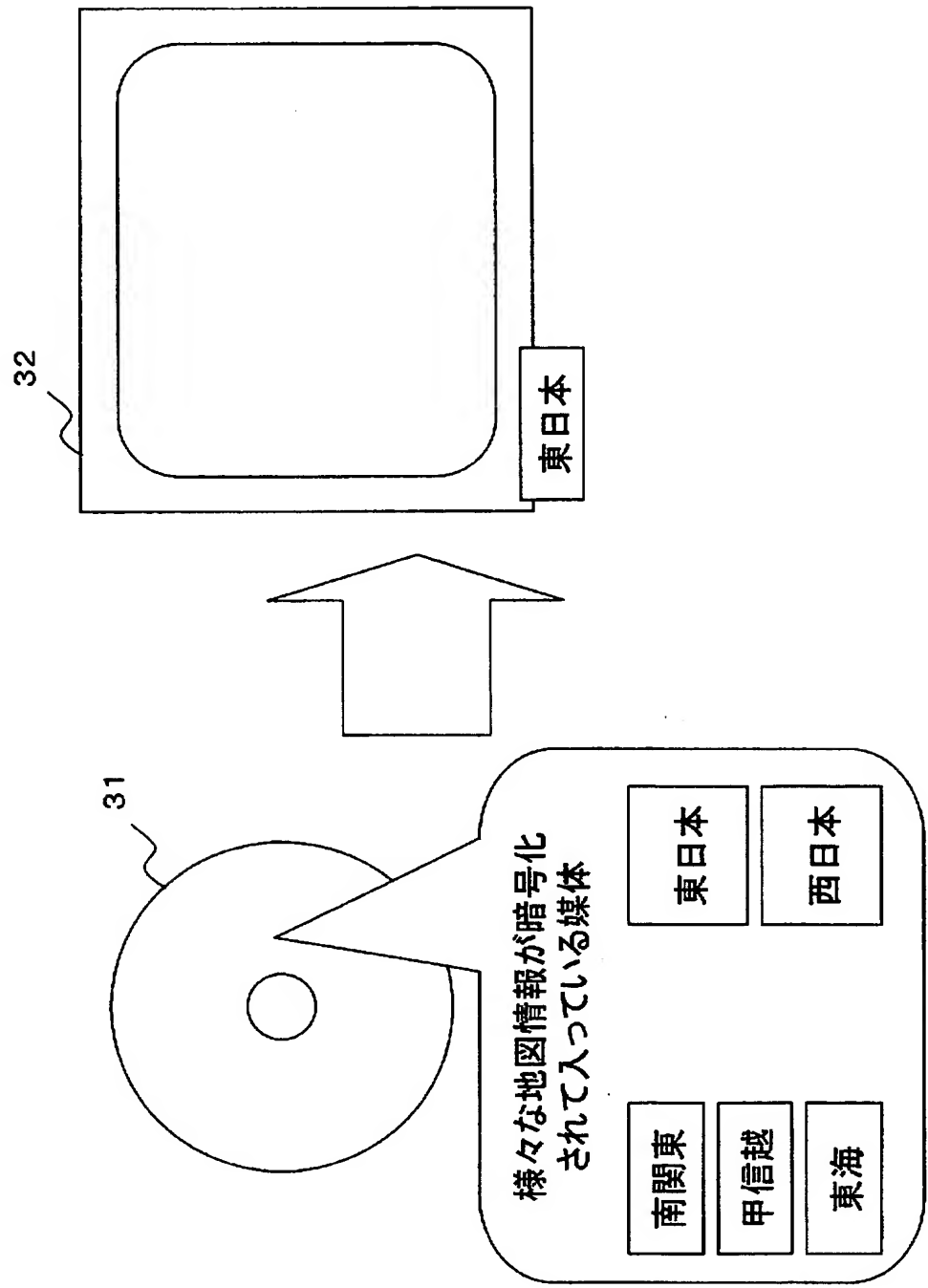
【図 18】

第4の実施の形態の暗号化された
地図データを開く処理のフローチャート



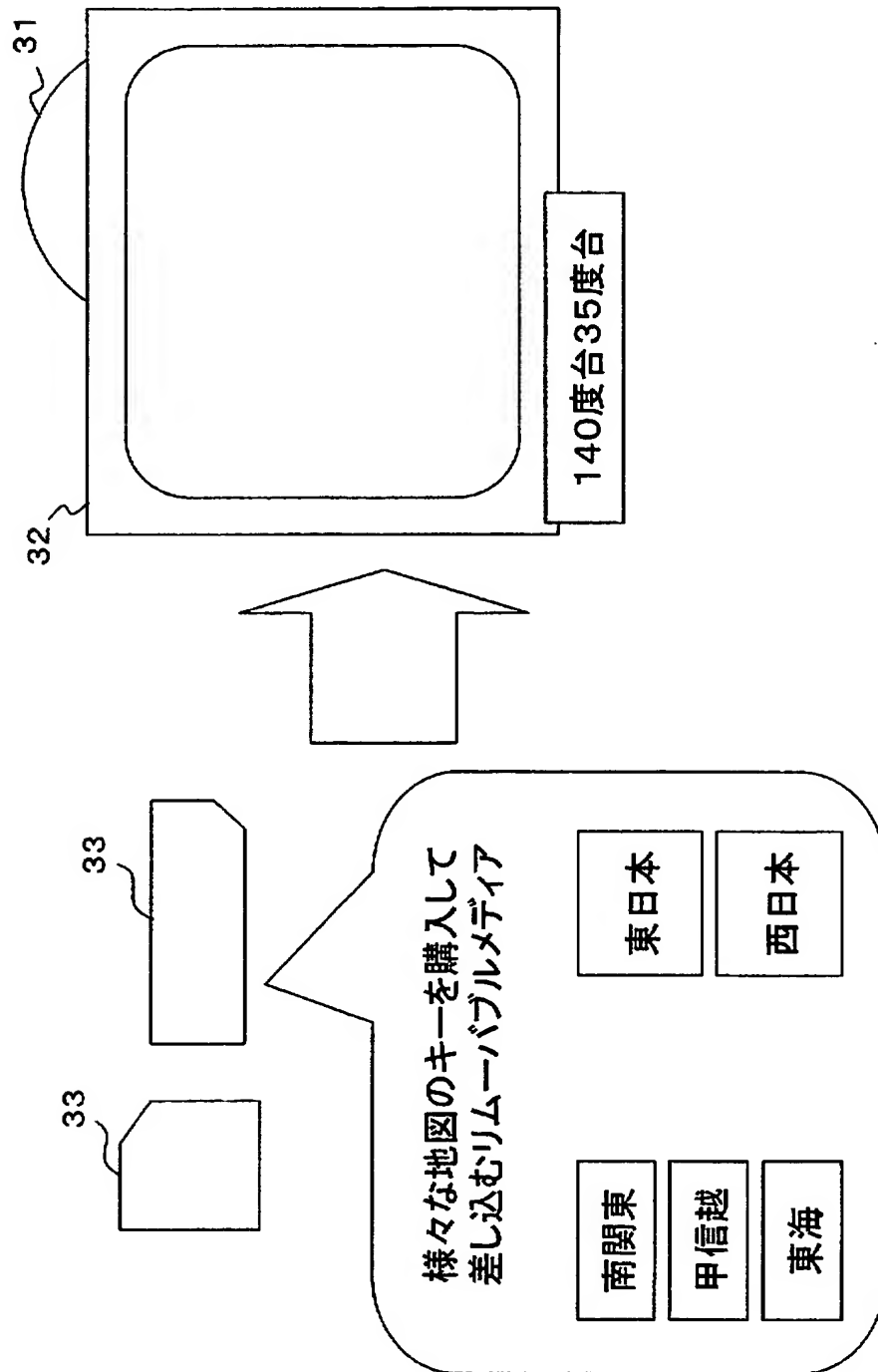
【図 19】

地図情報を記録媒体に記録した場合の説明図

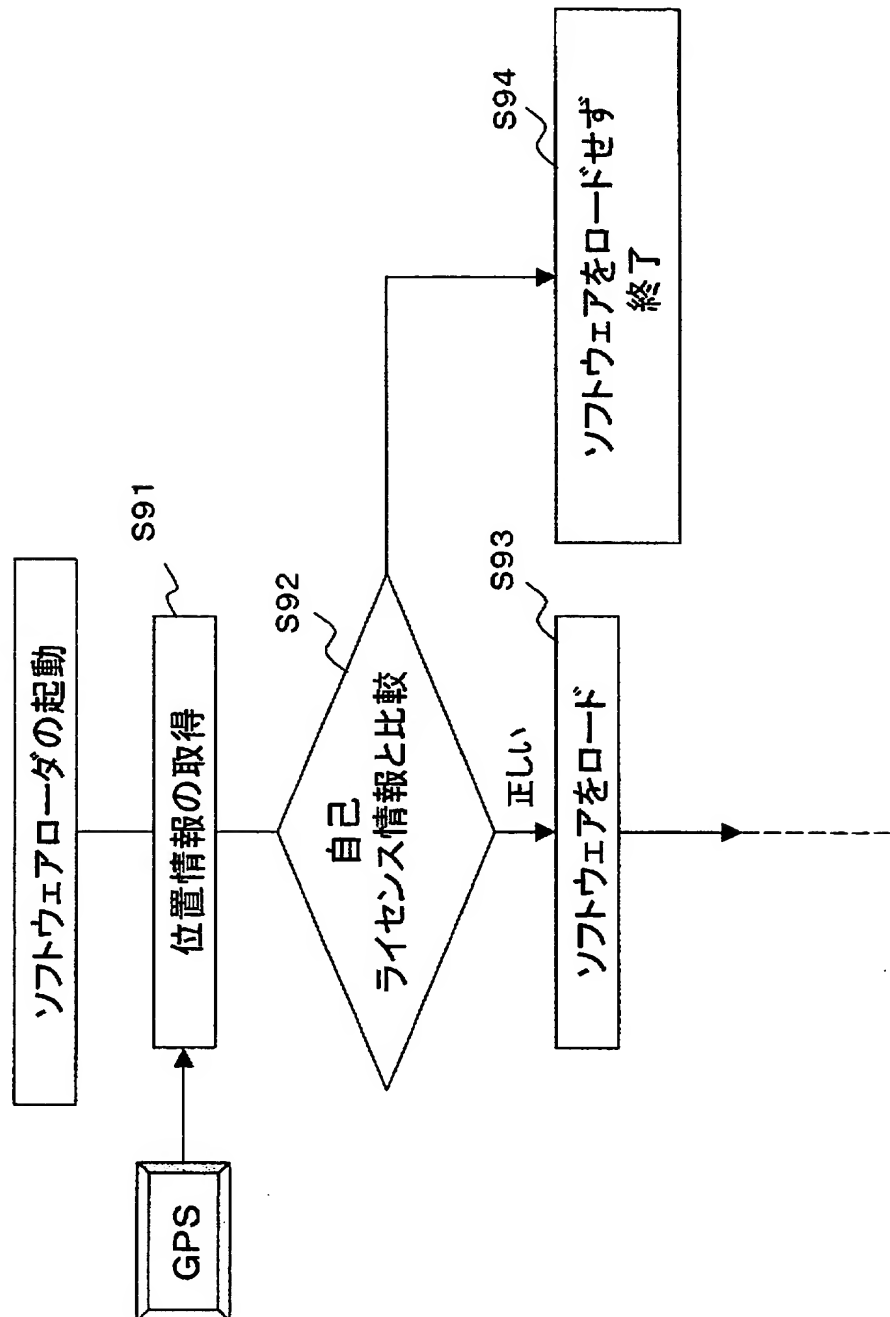


【図 20】

リムーバブルメディアに
アクセスキーを保存した場合の説明図

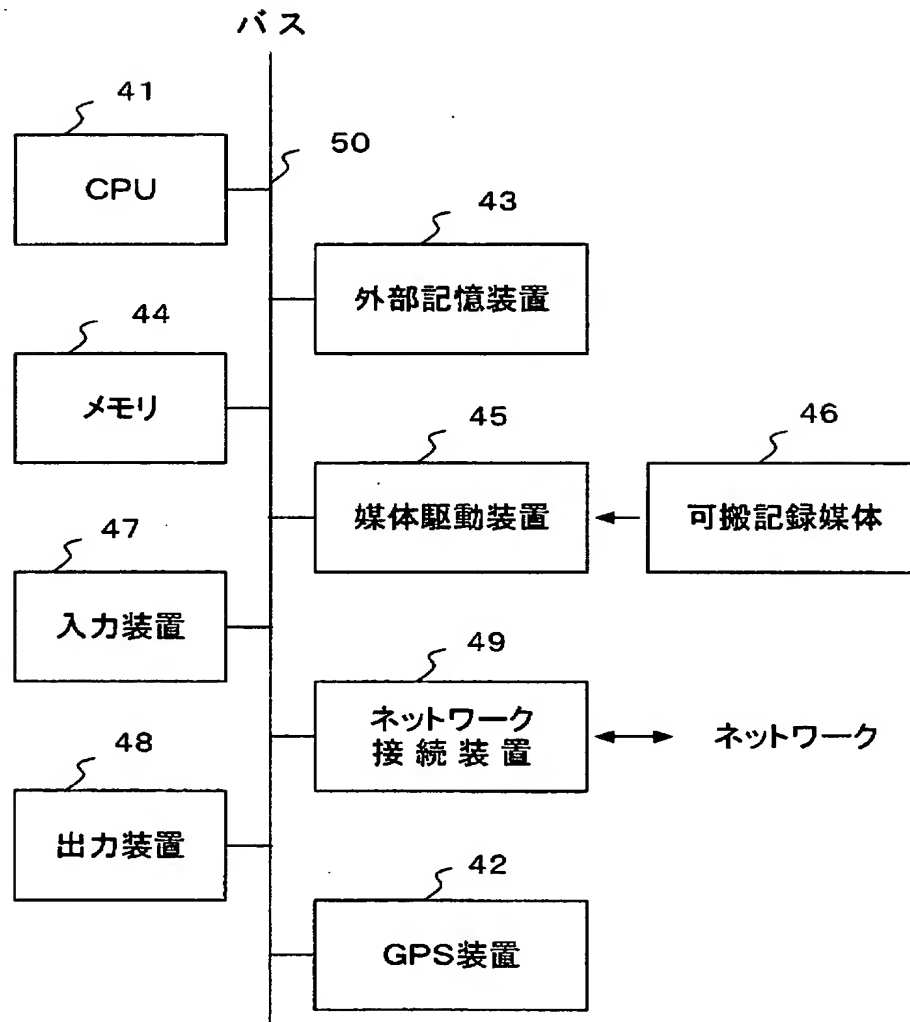


【図 21】

第5の実施の形態のライセンス保護ファイル
の実行処理のフローチャート

【図 22】

情報処理装置の構成図



【書類名】 要約書

【要約】

【課題】 指定した場所以外ではファイルを開くことができないようにすることである。

【解決手段】 G P S 装置から位置情報を取得し（図 4， S 1 1）、暗号化レベルに応じて位置情報にフィルタをかける（S 1 2）。フィルタをかけた位置情報をキーとしてデータを暗号化する（S 1 4）。ヘッダ及びダイジェストを作成し（S 1 5）、それらのデータを保存する（S 1 6）。位置情報により暗号化されたファイルを開くためには、保存時に指定された位置情報により復号する必要があるので、指定された場所以外ではファイルを開くことができない。

【選択図】 図 4

特願 2 0 0 3 - 0 9 5 7 2 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1 . 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社